




DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT SYSTEM CHANGE CONTROL FOR THE DEPARTMENT OF MENTAL HEALTH MANAGEMENT INFORMATION SYSTEM	POLICY NO. 1200.06	EFFECTIVE DATE 11/01/1999	PAGE 1 of 8
APPROVED BY:  Director	SUPERSEDES 302.15 11/01/1999	ORIGINAL ISSUE DATE 11/01/1999	DISTRIBUTION LEVEL(S) 1

PURPOSE

- 1.1 To provide Department of Mental Health (DMH) policy regarding the protection of Los Angeles County information, data, and information processing resources for system maintenance and enhancement requests.
- 1.2 To establish uniform guidelines in the prevention of fraud, embezzlement, and other abuses which take advantage of an individual's restricted access to the Mental Health Management Information System.
- 1.3 To specify standards in the protection of Mental Health data and information from loss, unauthorized use, modification, disclosure, or reproduction and to ensure the implementation and promotion of compliance with controls, standards and procedures.

SCOPE

- 2.1 Periodically, during the life cycle of an information system, modifications are necessary. These modifications are made necessary because of changes in internal operations of the organization, competitive demands, regulatory requirements, and the introduction of new information system technology. Whatever the reason for the changes, they must be documented and strictly controlled to prevent fraudulent and inadvertent modification.

RESPONSIBILITY

- 3.1 The DMH Chief Information Office (CIO) Division Chief, Systems Management Division, is responsible for ensuring that this policy is communicated to all CIO



**LAC
DMH**
LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH

DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
SYSTEM CHANGE CONTROL FOR THE DEPARTMENT OF MENTAL HEALTH MANAGEMENT INFORMATION SYSTEM	1200.06	11/01/1999	2 of 8

employees and other personnel authorized to access data and information. The Information Systems Security Administrator interprets and monitors this policy.

POLICY

- 4.1 All computer communications systems used for production processing must employ a formal change control procedure which is used to ensure that only authorized changes are made. This change control procedure must be used for all significant changes to software, hardware, and communications links.
 - 4.1.1 Before development (programming) of the system is authorized, management must be assured that the system design satisfies the user/manager requirements and incorporates the control requirements. The design review must be documented and be available for examination.
 - 4.1.2 Before being used for production processing, new or substantially changed business application systems must receive written approval from the CIO Division Chief, Systems Management, CIO Security Administrator, and, in some instances, the user/manager (at the level of Program Head and above), for the controls to be employed.
 - 4.1.3 Documentation reflecting all significant changes to production, computer, and communications systems must be prepared within a week from the time that a change took place. This documentation must reflect the proposed change, management approval, and the way in which the change was performed.
 - 4.1.4 For each system, a systems control procedure must be developed to ensure that all appropriate safeguards are incorporated into the system, tested before implementation, and tested periodically after implementation.



**LAC
DMH**
LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH

DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
SYSTEM CHANGE CONTROL FOR THE DEPARTMENT OF MENTAL HEALTH MANAGEMENT INFORMATION SYSTEM	1200.06	11/01/1999	3 of 8

- 4.1.5 Periodic reviews of production operating systems should be conducted to ensure that only authorized changes have been made.

SECURITY MEASURES

- 5.1 Whenever a computer-based process involves sensitive, valuable, or critical information, the system must include controls involving a separation of duties or other compensation control measures. These control measures must ensure that no one individual has exclusive control over this type of information assets.
- 5.1.1 Separation of duties is a key control that shall be applied to all development and modification of programs. All tasks involving sensitive, valuable, or critical information require at least two systems analysts and/or programmers from beginning to end to coordinate transactions. All transactions must be reviewed and approved by the CIO Division Chief, Systems Management, CIO Security Administrator, and, in some instances, the user/manager. No employee has the authority to approve his/her own work under any circumstances.
- 5.1.2 If procurement of third party software is being considered, management must obtain a written integrity statement from the involved vendor. This statement must provide assurances that the software in question does not contain undocumented features or hidden mechanisms that could be used to compromise the software's security, and will not require modification or abandonment of controls found in the operating system under which it runs.
- 5.1.3 Prior to being placed into production use, each new or significantly modified/enhanced business application system must include a brief security impact statement which has been prepared according to standard procedures.
- 5.1.4 DMH uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems. Individuals who violate this



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT SYSTEM CHANGE CONTROL FOR THE DEPARTMENT OF MENTAL HEALTH MANAGEMENT INFORMATION SYSTEM	POLICY NO. 1200.06	EFFECTIVE DATE 11/01/1999	PAGE 4 of 8
---	----------------------------------	--	---------------------------

policy will be subject to disciplinary action, including suspension, discharge from County service, termination of agreements, denial of service, and/or criminal and civil prosecution.

PROCEDURE

- 6.1 Each request for system modifications, new applications or subsystems to be developed must be submitted directly to the Chief Information Office for review and assignment to appropriate system staff.
- 6.2 Once a request is received, system staff will be responsible for the following:
 - 6.2.1 Coordination of production, including scheduling, timely distribution, and maintenance of required reports/logs/files.
 - 6.2.2 Review of current program specifications, data file elements and monitoring of testing structures prior to implementation.
 - 6.2.3 Review of all program inputs and outputs, including called or linked programs for potential impact to other processing.
 - 6.2.4 Discussion with qualified user representatives as to the change required reasons; therefore, and impacts to their operations.
 - 6.2.5 Training users on new subsystems, screens, procedures and reports.
- 6.3 All requests are grouped in the following categories, with priority one being the highest.

TYPE OF REQUEST

PRIORITY

Production Maintenance	1
System Operations	1
Quality and Scope of Client Care	2



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
SYSTEM CHANGE CONTROL FOR THE DEPARTMENT OF MENTAL HEALTH MANAGEMENT INFORMATION SYSTEM	1200.06	11/01/1999	5 of 8

Federal and/or State Regulations	2
Revenue Generation	2
Audit Findings	3

System Enhancements (which improve productivity and/or save costs)	3
Ad Hoc's (requiring vendor programming)	4
System Modifications (when what is currently taking place is acceptable or can be accomplished without vendor resources)	5

6.4 Upon completion of analysis, system staff will initiate a Maintenance Request (Attachment I) or a Service Request (Attachment II). These requests are issued when the business requirements of an existing system are changed or a new system is designed.

6.5 Maintenance Request

6.5.1 A Maintenance Request (MR) is generated when problems in production processing or hardware operation are encountered. If the problem detected affects the on-line applications, a bulletin will be posted on the Help Desk screen notifying the end-users of the problem and an estimated date and time as to when the problem will be resolved.

6.5.2 The system analyst will generate an MR, which includes the following information:

- 6.5.2.1 Date of Request
- 6.5.2.2 Type of Request – (New, Revision, Cancel)
- 6.5.2.3 Type of Problem – (on-line, Batch)
- 6.5.2.4 Fiscal Year
- 6.5.2.5 SMR Log Number
- 6.5.2.6 Problem Description – a brief description of the problem, requested change and the reasons required



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
SYSTEM CHANGE CONTROL FOR THE DEPARTMENT OF MENTAL HEALTH MANAGEMENT INFORMATION SYSTEM	1200.06	11/01/1999	6 of 8

- 6.5.2.7 End User's Signature
- 6.5.2.8 System Analyst Signature
- 6.5.2.9 Division Chief, Systems Management, Signature
- 6.5.2.10 Security Administrator Signature
- 6.5.2.11 Attachments
- 6.5.2.12 Corrective Action
- 6.5.2.13 Contract (Programmer) Signature
- 6.5.2.14 Contract Manager Signature
- 6.5.2.15 Date

- 6.5.3 The system analyst will investigate the causes of the problem and determine how long it will take to solve. If the problem cannot be resolved in five business days, the system analyst will provide a Status Report (Attachment III) to the CIO Division Chief, Systems Management, and the user/manager on a monthly basis.
- 6.5.4 Once management approval has been received, the system analyst will prepare and submit the MR to support staff to be entered onto the Problem Maintenance Log, photocopied and filed numerically, by request number, into the log book. The original MR is then forwarded to the programmer for processing.
- 6.5.5 Upon resolution of systems/production problems, the programmer will complete the MR, defining the problem, and the action taken to resolve the problem, including supporting documentation. The programmer will submit the MR to the system analyst for testing approval.
- 6.5.6 Upon completion of satisfactory systems tests, the system analyst will submit an Acceptance Review Sheet (Attachment IV) for the CIO Division Chief, Systems Management and user/manager review and approval to authorize program migration to production.



**LAC
DMH**
LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH

DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
SYSTEM CHANGE CONTROL FOR THE DEPARTMENT OF MENTAL HEALTH MANAGEMENT INFORMATION SYSTEM	1200.06	11/01/1999	7 of 8

6.5.7 Once signatures have been received, the MR will be entered into the Maintenance Request Log as completed and filed with the specification/testing documentation and reports.

6.5.8 Upon review, if program modifications are necessary to correct the problem, the system analyst will prepare a Service Request (SR). The Maintenance Request will be logged as a transfer for service request.

6.6 Service Request

6.6.1 A Service Request (SR) is generated when a request for system modification, new application or a subsystem is needed.

6.6.2 The system analyst will generate the SR requesting the following information:

- 6.6.2.1 Date of Request
- 6.6.2.2 Service Request Indicator – (New, Revision, Cancel)
- 6.6.2.3 Fiscal Year
- 6.6.2.4 Requestor Organization Name
- 6.6.2.5 Main Account No. (A20500)
- 6.6.2.6 SSR Number
- 6.6.2.7 MAPS Code (TQP)
- 6.6.2.8 Title of Request
- 6.6.2.9 Priority Level
- 6.6.2.10 End User, Phone Number
- 6.6.2.11 System Analyst
- 6.6.2.12 Problem Description
- 6.6.2.13 Signature of Authorized Representative

6.6.3 The system analyst will investigate the request and determine how long it will take to complete. A Status Report (Attachment III) to the CIO Division Chief, Systems Management, and the user/manager will be generated on a monthly basis.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
SYSTEM CHANGE CONTROL FOR THE DEPARTMENT OF MENTAL HEALTH MANAGEMENT INFORMATION SYSTEM	1200.06	11/01/1999	8 of 8

- 6.6.4 Once management approval has been received, the system analyst will prepare and submit the SR to support staff to be entered onto the Service Request Log, photocopied and filed numerically, by request number, into the log book. The original SR is then forwarded to the programmer for processing.
- 6.6.5 The contract programmer will complete the SR, defining the requirements and the action taken, including supporting documentation. The programmer will submit the SR to the DMH system analyst for testing approval.
- 6.6.6 The system analyst will review the system test results with the programmer.
- 6.6.7 Upon completion of satisfactory system tests, the system analyst will submit an Acceptance Review Sheet (Attachment IV) for the CIO Division Chief, Systems Management, and user/manager review and approval to authorize program migration to production.
- 6.6.8 The SR will be entered into the Service Request Log as completed and filed with the specification/testing documentation and reports.

AUTHORITY

Auditor-Controller Internal Control Certification Program (ICCP) Requirements, 1999

ATTACHMENTS

Attachment I	Maintenance Request Form
Attachment II	Service Request Form
Attachment III	Status Report Form
Attachment IV	Acceptance Review Sheet